METHOD AND SYSTEM FOR PROCESSING PASSWORD INPUTTED BY THE MATCHING OF CELLS

Technical Field

The present invention relates to a password system, and in particular to a method and system for processing a password inputted by the matching of cells that are capable of preventing a password from being revealed to the others in such a manner that a password inputted by a certain person is not known to others even when another person watches a password input procedure.

Background Art

A user authentication system has been widely used in various industrial fields for checking a certain user. The user authentication system is directed to performing a user authentication process using information provided by a user and information stored in a system. As information used for a user authentication, there are information memorized by a user such as ID and password, information stored in a storing medium such as a RF card, magnetic card, etc., and a biological information implemented using a physical feature such as a fingerprint, an iris, face, etc.

Among the above methods, the password system is a user authentication system implemented using information memorized by a user. It is easy to use the same, and the cost is lower as compared to other user authentication systems. The password system is easily implemented. Therefore, the password system has been most widely used.

Generally, the password system is formed of a system related module for a user authentication process, and a user interface related module for inputting an ID or password. The modules having an encoding function are selectively used based on the system. A password system of a single user system like a desktop-alone, cellular phone, etc. does not include a password module or other security platform module.

A password system having a plurality of users like an Internet banking system and UNIX system includes a password module or other security platform module each implemented based on an open key structure.

The password system is one of user authentication system most commonly used based on the above-described advantages. However, the password system has a very big problem that an input procedure of password may be revealed to others. In order to prevent the above problems that the password is revealed to others while being inputted by a user, the following technologies are disclosed.

According to the Japanese patent laid-open No. Hei 5-334334 by Kijima Katshuiro made open December 17, 1993, in a password input apparatus, a password input unit is changed in such a manner that a user selects a certain patch pattern with respect to a password input number row, and a number row is moved from a reference pattern. According to the Japanese patent laid-open No. 2000-339084 by Ono Kazuhiko made open December 8, 2000, in a password system capable of changing an input pattern, when a user selects a certain cell, the selected cell is matched with a cell including a password symbol provided in a reference board based on a computation. According to the Japanese patent laid-open No. Hei 9-274531 by Kishimoto Takuya made open October 21, 1997, in a password input system, a key input alignment is changed to prevent a reveal of password. According to the Japanese patent laid-open No. Hei 2000-214943 by Ariga Toshihiro made open August 4, 2000, there is provided a method for changing a password input unit capable of preventing a reveal of password even when a password input procedure is open to others. In addition, according to the Japanese patent laid-open No. 2001-350590 by Hiromachi Akihisa made open December 21, 2001, there is provided an input apparatus in which a key input cell is randomly changed so that others do not know a user password input procedure.

According to the above disclosed techniques, since a key alignment

position of a key input apparatus is fixed, even when a third party person recognizes only the position of a key alignment inputted by a password input person, the inputted key value is easily known to others. In addition, since the randomly changed key alignments are opened to others positioned near a password input person, the password is directly revealed to others. In addition, there are further methods for providing many images on a user interface, and then the images are sequentially selected by the user. In the above method, it is impossible to memorize a long password. Therefore, the above methods cannot basically overcome the revealing problems of password.

Disclosure of Invention

Accordingly, it is an object of the present invention to provide a method and system for inputting a password based on a cell matching method capable of preventing a revealing of password by preventing others from knowing the inputted password even when a user's password input procedure is directly watched to others.

In order to achieve the above object, a password system according to the present invention includes a reference board and a matching board on a user interface. The reference board and matching board each are formed of at least more than two cells. The matching board reacts with respect to a user or a

system computation. The reference board does not react with respect to a user and a system computation. The cell in the matching board and the cell in the reference board may be matched by a user or a system. The cell in the matching board and the cell in the reference board may be concurrently matched in multiple numbers. In a method of the present invention, the user selects a cell in the matching board, and the selected cell is matched with the cell having a password symbol in the reference board for thereby inputting a password. In another password input method of the present invention, the system selects a cell in the reference board matched with the cell including the password symbol in the matching board from the matched matching board and reference board for thereby inputting a password.

To achieve the above objects, there is provided a password system, comprising a display unit having a reference board in which a plurality of cells including one real reference cell that is a reference for matching, and a plurality of cells including a plurality of virtual reference cells for disguising the real reference cell are aligned and displayed, and a matching board in which a plurality of cells having one real matching cell matched with the real reference cell and a plurality of virtual matching cells for disguising the real matching cell are aligned and displayed; a cell generation unit for generating a group of cells displayed on the reference board and the matching board; a display control unit

for receiving information concerning a group of the cells generated by the cell generation unit and aligning and displaying on the reference board and the matching board; a matching unit for matching a real reference cell and a real matching cell so that a user inputs a password; a matching cell process unit for generating a group of matched cells when the symbols aligned on the reference board and the matching board are matched by the matching unit and inputting into an authentication process unit; a memory for storing an authentication reference information; and an authentication process unit for performing an authentication process for judging whether a real matching cell is matched with a real reference cell included in the group of the matched cells based on an authentication reference information and permitting or denying an access to the main system by the user.

To achieve the above objects, there is provided a user authentication method of a password system, comprising the steps of a step for generating a first cell group including one real reference cell that is a reference for matching and a plurality of virtual reference cells for disguising the same, and a second cell group including one real matching cell matching with the real reference cell and a plurality of virtual matching cells for disguising the same; a step for displaying a reference board for displaying the first cell group and a matching board for displaying the second cell group on a display unit; a step for inputting

a two-password for matching the real reference cell of the reference board and the real matching cell of the matching board by a matching unit; a step for generating a group of the matched cells when the symbols of the reference board and the matching boards are matched and inputting into an authentication process unit; and a step for performing an authentication process for allowing or denying an access to a main system by a user based on the authentication reference information for the authentication process and the inputted matched symbol group.

In the password system according to the present invention, even when others watch a password input procedure, the others do not know the cell matched with a cell including a password among a plurality of matched cells of the matching board and reference board, so that it is impossible to know the password even when others watch the password input procedure.

Brief Description of Drawings

The present invention will become better understood with reference to the accompanying drawings which are given only by way of illustration and thus are not limitative of the present invention, wherein;

Figures 1 through 27 are views for describing a first embodiment of the present invention;

Figure 1 is a view illustrating various expression types of a cell;

Figure 2 is a view illustrating various expression types of a board;

Figure 3 is a view illustrating an example of a method for mapping a certain board to a straight line shaped board;

Figure 4 is a view illustrating an example of overlapped cells;

Figure 5 is a view illustrating an example that two boards are overlapped;

Figure 6 is a view illustrating an example that four boards are overlapped;

Figure 7 is a view illustrating a condition that overlapped cells should satisfy;

Figure 8 is a view illustrating an example that at least more than one board are moved in the same direction by the same distance;

Figure 9 is a view illustrating an example that at least more than one board are concurrently not shown on the user interface;

Figure 10 is a view illustrating an example that a board reacts with respect to a computation for a board, and a board does not react with respect to the computation;

Figure 11 is a view illustrating an example for describing a reference board formed of at least more than two boards;

Figure 12 is a view illustrating an example for describing that a cell in a

matching board is matched with a cell in a reference board by performing a computing with respect to a matching board;

Figure 13 is a view illustrating an example for describing a cell including a password symbol;

Figure 14 is a flow chart of a procedure that the password symbols are sequentially matched with one cell in a matching board for thereby inputting a password;

Figure 15 is a view illustrating an example that there is a cell in a matching board, which is not matched with a cell (cells) in a reference board when a computation is performed with respect to a matching board so that the cell in the matching board selected by a user is matched with the cell having the password symbols;

Figure 16 is a view illustrating an example for describing a rotational movement using an imaginary reference board;

Figure 17 is a view illustrating the construction that an imaginary reference board is a straight line;

Figure 18 is a view illustrating an operation that a rotational movement is possible without an imaginary reference board;

Figure 19 is a view illustrating the construction that an imaginary reference board and a reference board are combined and recognized as one

reference board;

Figure 20 is a flow chart of a method that a system recognizes the cell selected by the user in the case that the system knows the length of password;

Figure 21 is a view illustrating the construction that a special symbol is shown in a reference board;

Figure 22 is a flow chart of a method that a system is enabled to know a cell that the user selects in the case that the system does not know the length of password;

Figure 23 is a flow chart illustrating a procedure that the system determines a password inputted by a user based on a method that the system knows the length of password in a method that the cell selected by a user in the matching board is matched with a password symbol in the reference board for thereby inputting a password;

Figure 24 is a view illustrating a procedure that the cell selected by the user in the matching board is matched with a password symbol in the reference board for thereby inputting a password;

Figure 25 is a view illustrating a procedure that a system determines one password;

Figures 26 and 27 are views illustrating another example of a first embodiment of the present invention;

Figure 26 is a view illustrating an example that a reference board and a matching board are aligned in parallel, so that the reference board and the matching board are not overlapped;

Figure 27 is a view illustrating an example that a straight line shaped matching board is overlapped with a matrix shaped reference board;

Figures 28 through 33 are views for describing a second embodiment of the present invention;

Figure 28 is a flow chart of a procedure that a cell in the reference board matched with a password symbol in the matching board is selected for thereby inputting a password in the case that a system knows the length of password;

Figure 29 is a flow chart of a procedure that a cell in the reference board matched with a password symbol in the matching board is selected for thereby inputting a password in the case that the system does not know the length of password;

Figure 30 is a view illustrating an operation that a matching board is disappeared on a user interface;

Figure 31 is a flow chart of an operation of a system in the case that a system knows the length of password;

Figure 32 is a view illustrating an example for describing a method that a system determines one password symbol in the case that a system knows the

length of password;

Figure 33 is a view illustrating an example that a reference board and a matching board are aligned in parallel, so that they are not overlapped as another example of a second embodiment of the present invention;

Figures 34 through 36 are views for describing a third embodiment of the present invention;

Figures 34A and 34B are views for describing a password input method according to a third embodiment of the present invention, of which Figure 34A illustrates a reference board and a matching board before matching, and Figure 34B illustrates a reference board and a matching board after matching;

Figure 35 is a view for describing a password input method according to a third embodiment of the present invention based on a set principle;

Figure 36A is a view illustrating a real image reference cell and an imaginary reference cell and a real image matching cell and an imaginary matching cell used in the reference board and matching board of Figure 34A;

Figure 36B is a view illustrating a real image matched RRC and RMC and an imaginary image matched VRC, VMC and MCG in the pairs of matched cells of Figure 34B;

Figures 37A through 37B are views of an example that two passwords are inputted by repeatedly performing a plurality of cell matching processes;

Figures 38A through 38D and Figures 39A and 39B are views of various examples for generating RMSG and RPSG from two passwords;

Figure 40 is a block diagram illustrating a relationship between a password system and a main system adapting the same according to a preferred embodiment of the present invention;

Figure 41 is a view illustrating the construction of a password system and a user interface according to the present invention;

Figure 42 is a flow chart illustrating a user authentication process of a password system according to the present invention;

Figure 43 is a view of a user interface in a main system according to an embodiment of the present invention;

Figures 44A through 44D are views illustrating various examples of a reference board and a matching board;

Figure 45 is a view illustrating an example that a reference board is omitted;

Figure 46 is a view illustrating another examples of a display type of a reference board and a matching board;

Figure 47 is a view illustrating another example for displaying at least more than matching boards in parallel;

Figure 48 is a view of an example of a graphic user interface capable of

providing an input window for inputting a forward movement distance of a reference board for a symbol matching;

Figure 49 is a view of an example of a graphic user interface having a plurality of input buttons for circulation-matching symbol rows;

Figure 50 is a view illustrating an example of a graphic user interface in the case that a matching board is automatically circulated;

Figure 51 is a view of an example of a user interface of a two-password system cooperating with an electronic circuit;

Figure 52 is a view illustrating another example that only one reference board is shown;

Figure 53 is a view of an example of a circuit construction of a user interface of Figure 51;

Figure 54 is a view of an example of a user interface of a password system cooperating with a mechanical mechanism;

Figure 55 is a view of an example of a circuit construction of a user interface of Figure 54;

Figure 56 is a view of an example that cells are aligned for adjusting a revolution of matching board within a certain range;

Figures 57A through 57D are views for describing an example of a set of matched cells;

Figure 58 is a view illustrating a table of a set of matched cells of Figures 57A through 57D;

Figure 59 is a flow chart of a detailed process of a password authentication process;

Figure 60 is a view illustrating the symbols of MCG matched with RMSG guided from a two-password;

Figures 61 and 62 are views of an example of authentication reference information stored in a memory;

Figure 63 is a view illustrating an example that a password system according to the present invention is mounted on a standalone system;

Figure 64 is a view illustrating an example that a password system according to the present invention is mounted on a main system based on a network; and

Figure 65 is a view illustrating an example that a password system is mounted in a communication terminal based on a network.

Best Mode for Carrying Out the Invention

The present invention provides a new password input method capable of preventing a revealing of password even when a password input procedure is shown to others and a user interface and a password system having a

password authentication process for the above method.

1. First embodiment – password system for inputting password by matching a certain cell and a specific cell

1) Definition of cell and board

The basic unit of information shown to a user on a user interface of a password system according to the present invention is called as a cell. Figure 1 is a view showing various cells. (a) shows a cell of 3. (b) shows a cell having a solid line rim and a transparent rectangular shape interior. (c) is a gray color rectangular cell.

The set of cells is called as a board. Here, in the present invention the terminology "set" represents a common set. The board may be shown in various shapes on a user interface. Figure 2 is a view illustrating various shapes of boards. As shown in Figure 2, (a) shows a rectangular board having nine cells formed in a matrix shape. (b) shows a circular board formed of eight cells. (c) shows a board formed of six scattered cells. (d) shows a board formed of seven scattered number cells. As not shown in the drawings, a board may be formed of a plurality of cells in a straight line. The dotted lines in (c) and (d) are provided for simply figuring out a shape of a board. The dotted lines are not shown in an actual user interface.

The shape of the board may be commonly formed. Assuming that a board formed of an n-number of cells is X, and a board formed of a n number of straight line shaped cells is Y, a sequence is provided to the cells in X, and the cell having an i-th sequence in X may correspond with the i-th cell of Y ($1 \leq l \leq n$). Therefore, in the present invention, when a board is mapped in a straight line shape, it is recognized as a board irrespective of the number and shape of the cells and a state that the same cells are overlapped or not. For example, Figure 3B is a view showing the construction that a sequence is provided to the cells of the board, and Figure 3C is a view showing the construction that the cell having i–th sequence of Figure 3B corresponds to the i-th straight line shaped cell.

2) Display of cell and board

At least more than two cells may be overlapped and shown on the user interface. For example, Figure 4C is a view showing the construction that the cells of Figures 4A and 4B are overlapped. Since the cells may be overlapped and shown on user interface, the cells may be overlapped and shown on the board or user interface. For example, Figure 5C is a view showing the construction that the board of number cells of Figure 5A is overlapped with the board formed of rectangular cells of Figure 5B. As shown in Figures 5A and 5C, the dotted lines surrounding the board formed of number cells are formed for

only figuring out the shape of the board and are not actually shown on the user interface.

When the boards are overlapped, only two boards are not overlapped. Namely, at least more than three boards may be overlapped. For example, Figure 6E is a view showing the construction that the boards of Figure 6B are overlapped. Figure 6F is a view showing the construction that the board of Figure 6C is overlapped with the board of Figure 6D. Figure 6G is a view showing the construction that two overlapped boards of Figure 6E are overlapped with two overlapped boards of Figure 6F. The dotted lines of Figures 6A, B, C, D, and E are formed for only figuring out the shape of the board and are not actually shown in the user interface.

Assuming that overlapped two boards are A and B, each cell of the board A and each cell of the board B are overlapped, and the entire construction is visually seen. For example, as shown in Figure 7E in which four cells of Figures 7A, B, C, and D are overlapped, the cell of Figure 7A and the cell of Figure 7C are fully seen at one cell, and the cell of Figure 7B and the cell of Figure 7D are partially seen.

In the present invention, it is assumed that at least more than two cells of B are not concurrently overlapped with one cell of A. For example, Figure 6G is a view showing the construction that four boards are overlapped. Namely, at

least more than two cells in another board are not overlapped with one cell of one board. At this time, when the rims of two cells are abutted, it is recognized that they are not overlapped.

3) Computation of boards

In the present invention, at least more than one board shown on the user interface can be concurrently moved in the same direction by the same distance. For example, Figure 8D is a view showing a result that the boards of Figures 8A and 8B are moved in the same direction by the same distance in a state of Figure 8C. As shown in Figure 8D, the boards in the original position before the movement are not shown on the user interface after the boards are moved. For easier understanding, the above boards are shown. In addition, the dotted lines of Figures 8A, B, C, and D are shown for only figuring out the shape of the board and are not actually shown on the user interface.

At least more than one board may not be concurrently shown on the user interface. Figure 9F is a view showing a state that the boards of Figures 9A and 9B are disappeared from the state of Figure 9E in which the boards of Figure 9A, B, C and D are overlapped. The dotted lines of Figure 9A, B and C are formed for only figuring out the shape of the board and are not actually shown on the user interface.

In the present invention, the user or system computes with respect to the boards for inputting symbols belonging to the password. At this time, the computation means that the board is changed from the previous state to the next state. For example, when the boards are moved or disappeared, it is recognized as a result of the computation. At this time, it is recognized that the boards having the same states after or before the user or system performs a computation are not affected by the computation. For example, the arrows of Figure 10F represent that the boards of Figures 10A and 10B are moved from the states of Figure 10F in which the boards of Figure 10A, B, C and D are overlapped. Figure 10G is a view showing the construction that the boards of Figures 10A and 10B are moved. In the construction of Figure 10G, the boards of Figure 10C and 10D are not moved. Therefore, in this case, the boards of Figures 10A and 10B are not affected by the computation. The boards of Figure 10A and 10B are not affected by the computation. The dotted lines of Figures 10A, 10B and 10C are formed for only figuring out the shape of the board and are not actually shown on the user interface.

4) Definitions of matching board and reference board

When a computation is performed with respect to the boards for inputting the symbols belonging to the password, the set formed of boards

reacting with respect to the computation in the same manner is called as a matching board, and the set formed of the boards not reacting with respect to the computation is called as a reference board. For example, in the example of Figure 10G, the boards of Figure 10Aand Figure 10B react with respect to the computation and are moved in the same distance by the same distance. Therefore, the set formed of the boards of Figure 10A and Figure 10B is called as a matching board, and since two boards of (c) and (d) of Figure 10 do not react with respect to the computation, the set formed of two boards of Figure 10C and 10D is called as a reference board.

The reference board is formed of at least more than one board, but it is recognized as one board. For example, assuming that the board of Figure 10C is called as a reference board, even when the board of Figure 11C is overlapped with the boards of Figure 11A and Figure 11B, the boards are recognized as one board. Therefore, in the case that the reference board is formed of at least more than two boards, and at least more than two cells in at least more than two boards are overlapped, the overlapped cells are set as one and are recognized as one cell in the reference board. Similarly, the matching board is formed of at least more than one board, but it is recognized as one board. In addition, in the case that the matching board is formed of at least more than two boards, and at least more than two cells in at least more than

two boards are overlapped, the overlapped cells are set and recognized as one cell in the matching board.

5) Movement of board, and matching of cell

The user can overlap a certain cell in the matching board and a certain cell in the reference board by performing a computation with respect to the matching board. When the cell in the matching board is overlapped with the cell of the reference board, it is called that the cell of the matching board is matched with the cell of the reference board. For example, assuming that the board of Figure 12A is called as a matching board, and the board of Figure 12B is called as a reference board, Figure 12D shows the case that a certain cell of the matching board is matched with a certain cell of the reference board in the state of Figure 12C. The cell having a thick boundary line in Figure 12C represents a certain cell in the reference board and a certain cell in the matching board that the user wants match.

Assuming that the user's password is $P_1 P_2 \ldots P_n$, P_1 is cell but is called as a password symbol ($1<l<n$). In addition, the cell overlapped with the password symbol and the password symbol in the reference board or matching board are combined and called as a cell including the password symbol. For example, assuming that Figure 13A shows the matching board, and password

symbol is 1, Figure 13B shows the cell including 1. At this time, if there is not a cell overlapped with the password symbol in the matching board or the reference board, the password symbol itself is called as the cell including the password symbol. For example, assuming that Figure 13C shows the reference board, and the password symbol is 1, Figure 13D shows the cell including 1.

Figure 14 is a flow chart of a procedure that the password symbols in the reference board are sequentially matched with one cell in the matching board for thereby inputting a password.

As shown therein, assuming that the user's password is $P_1P_2, \ldots P_n$ ($I<I<n$), the system shows the matching board and the reference board on the user interface (S101). The user selects a certain cell in the matching board (S102). The user repeatedly performs the process for performing a computation with respect to the matching board so that the cell selected in the step S102 is matched with the cell included in P_I (S103 through S106). The user transfers a password input completion signal to the system (S107).

In the method of Figure 14, it is not limited that the user selects a certain cell in the matching board one time, and the system is not limited to show the reference board and the matching board one time. For example, the user can repeatedly perform the process that the user selects a certain cell in the matching board, and the selected cell is matched with the cell including the

password symbol. The system can show a new reference board and a matching board on the user interface whenever one cell selected by the user in the matching board is matched with one cell including the password symbol before the user completes inputting the password.

In the method of Figure 14, the step S107 may be omitted in the case that the system knows the length of the password.

In the method of Figure 14, when the cell in the matching board selected by the user is matched with the cell including the password symbol in the reference board, the cell in the matching board that the user did not select should be matched with the cell including the symbols, the password symbol. All cells in the matching board are matched with the cells in the reference board, so that others who do not know the cells in the matching board selected by the user cannot know the user's password symbols even when others see the input procedure of the password symbols.

In the method of claim 14, since the cell selected by the user should be matched with the cell including the password symbol in the reference board, there should be cells including at least password symbol in the reference board. For example, assuming that the password symbols are numbers from 0 to 9, the reference board should include the cells including at least numbers from 0 to 9.

In the method of Figure 14, the password symbols in the matching

board are preferably shown in a certain recovery extraction sequence. Even when they are not sequentially shown, there is no problem. Since the user select a certain cell in the matching board, it is not needed that all cells in the matching board should be different. However, in the case that all cells are same, the user may confuse with the selected cell, so that it is not preferred that all cells are same.

In the step S102 of Figure 14, what the cell selected by the user is matched with the cell including the password symbol P_i in the reference board may be implemented using an input apparatus. For example, the matching board is recognized as a cursor, and the user drags the matching board and drops the same when the cell selected by the user is matched with the cell including P_i in the reference cell.

In the method of claim 14, the step S107 may be omitted in the case that the system knows the length of the password. Namely, since the system knows the length of the password, when the user performs the step S104 by n-times, the system recognizes that the password input is completed. In the case that the system does not know the length of the password, the user transfers a signal that the password input is completed to the system using an input apparatus. For example, the user pushes a left button of the mouse for performing the step S104 and pushes a right button of the mouse for performing

the step S107.

In the method of Figure 14, when the cell selected by the user in the matching board is matched with the cell including the password symbol in the reference board, as it was described earlier, the cells, not the cells selected by the user, in the matching board should be matched with the cells including the symbols, not the password symbol, in the reference board. At this time, in the case that a computation is performed so that the cells in the matching board selected by the user are matched with the cells including the password symbol, there may be the cells of the matching board not matching with the cells in the reference board.

For example, assuming that Figure 15A shows the matching board, and the matching board of Figure 15B is moved in the direction of the arrow, Figure 15C shows that there are the cells in the matching board not matching with the cells in the reference board.

The above problems may be overcome by rotating the cells in the matching board out of the range of the reference board when the matching board is moved.

The rotation and movement will be described.

Assuming that Figure 15A shows the matching board, and the matching board is moved in the direction of the arrow of Figure 15B, eight imaginary

reference boards are placed on the surrounding portions of the reference board. Figure 16A shows the positions on which eight imaginary reference boards are placed. In Figure 16A, the rectangular shape means the reference board. Figure 16B shows the moving direction of eight imaginary reference boards and the matching board. The cells indicated by the dotted lines in Figure 16B are not actually shown on the user interface but are provided for describing the rotation and movement.

Figure 16C shows a result after the matching board is moved. As shown in Figure 16D, the cell in the imaginary reference board matched with the cell in the matching board in Figure 16C is recognized as the cell in the reference board, and the cells in the reference board not matching with the cell in the matching board is recognized as the cell in the reference board.

Figure 16E shows a result after the matching board is moved in the direction of the arrow. The movement of the matching board may be described using the imaginary reference board based on the shapes of the reference board and the matching board. The shape and number of the imaginary reference board may be different based on the computation with respect to the shape of the board and the matching board. For example, assuming that the rectangular cell indicated by the full line in Figure 17 is the cell in the reference board, and the computation with respect to the matching board is performed for

moving the matching board in the left and right directions, two imaginary reference boards indicated by the dotted line may be provided, and a result of computation will be described.

In a certain shaped board, it is possible to describe the computation with respect to the matching board without considering the imaginary reference board. For example, assuming that Figure 18A shows the matching board, and Figure 18B shows the reference board, in the case that Figure 18C concurrently shows the matching board and the reference board, the user can enable the matching board to rotate. Assuming that when the matching board of Figure 18A is rotated in the right direction 12 times, the same matching board as Figure 18A is obtained, Figure 18D shows a result that the matching board is rotated in the right direction one time. Therefore, Figure 18D shows a result of the computation performed with respect to the matching board without using the imaginary reference board. The dotted lines of Figures 18A, B and D are provided for simply figuring out the shape of the board and are not actually shown on the user interface.

When the computation is performed with respect to the matching board, in the case that the cell in the matching board is rotate and moved out of the range of the reference board, the user may visually feel inconvenient based on the shape of the matching board. The above problem may be overcome by

providing multiple reference boards. At this time, since multiple reference boards identically react with respect to the computation, the multiple reference boards are recognized as one reference board. For example, Figure 19 shows the case that nine reference boards are shown on the user interface. At this time, since nine reference boards identically react with respect to the computation, they are recognized as one reference board.

Since it is impossible to describe all possible shapes of reference boards and matching boards and all computations and results of the same, it is recognized that the reference board and matching board and computation of the same and results of the same are within the ranges that a person skilled in the art can understand.

In the method of Figure 14, when the user selects one cell in the matching board, the system does not know the user selected which cell. The method for overcoming the above problem will be described with reference to Figures 20 and 22.

Figure 20 is a flow chart of a method for enabling the system to know a user's selection of a certain cell when the system knows the length of password. Referring to Figure 20, assuming that the user's password is $P_1P_2...P_n$. The user repeats a process of matching the cell selected in the step S202 with P_l ($1<l<n$)(S204). Since the system knows the length of password, when the user

performs the step S204 n-times, at least more than one cell including the special symbol is transferred to the reference board (S207). Figure 21 is a view illustrating an example that there are special symbols * in nine cells in the reference board. The user matches the cell selected in the step S202 with a cell including the special symbol in the reference board (S208).

In the step S207, when the cell selected by the user in the matching board is matched with the cell including the special symbol in the reference board, the other cells including the special symbol in the reference board are not preferably matched with ant cell in the matching board.

Figure 22 is a flow chart of a method for enabling the system to know the user selects a certain cell in the case that the system does not know the length of password. Referring to Figure 22, assuming that the user's password is $P_1P_2...P_n$, the user repeats the process of matching the cell selected in the step S302 with P_I ($1<I<n$) (S307). The user transfers a signal that the step S304 is completed to the system (S307). The system shows at least more than one cell including a special symbol in the reference board (S308). The user matches the cell selected in the step S302 with the cell including a special symbol in the reference board (S309).

There may be various methods for recognizing that the system selects the cell for inputting the password. The method according to the present

invention is a preferred embodiment among multiple embodiments.

Figure 23 is a flow chart of a procedure that the system determined the password inputted by the user based on the method of Figure 20 in a method for inputting the password in such a manner that the cell selected by the user is matched with the password symbol in the reference board.

It is assumed that the system shows the reference board and the matching board on the user interface like Figure 24A, and the user selects the cell including the symbol of 8 in the matching board, and the system knows that the length of the password of the user is 4, and the user sequentially matches the cell including the symbol of 8 in the matching board with the cells including the symbols of 1, 5, 2, and 8 in the symbol board. Figure 24B shows that the cell having the symbol of 8 in the matching board is matched with the cell including the symbol of 1 in the reference board. Figure 24C shows that the cell including the symbol of 8 in the matching board is matched with the cell including the symbol of 5 in the reference board. Figure 24D shows that the cell including the symbol of 8 in the matching board is matched with the cell including the symbol of 2 in the reference board, and Figure 24E shows that the cell including the symbol of 8 in the matching board is matched with the symbol of 8 in the reference board.

It is assumed that the system shows the reference board formed of the

cells including the special symbols of Figure 24F on the user interface when the user completes matching the cell in the matching board with the cell including the password symbol in the reference board. Under the above assumption, the user matches the cell including the symbol of 8 in the matching board with the cell including the special symbol of the reference board. A result of the above operation is shown in Figure 24A. Referring to Figure 24F, the matching board is shown on the user interface, but the matching board is not shown for helping understanding.

The procedure that the system determines one password will be described with reference to Figures 24B, C, D, E and F.

The system stores the symbols in the cell of the matching board. At this time, the same two cells may appear in the matching board. The matching board may be mapped in a straight line shape. Since a certain sequence may be provided to the straight line board, the sequences provided to the cell may be recognized as the symbols. It is recognized that the cell of the matching board includes symbols.

Figure 25A shows an example that the symbols in the cell of the matching board are stored in one dimensional alignment formed of nine rooms.

Figure 25B shows a result that the symbol included in the cell in the reference board matched with each symbol included in the cell of the matching

board in Figure 24B is stored in the place in which the symbol included in the cell of the matching board is stored. It is recognized that the symbol in the same row as the symbol included in the cell in the reference board matched in Figures 25B, C, D, E and F is stored in the place in which the symbol included in the cell of the matching board is stored.

Figure 25C shows a result that the symbol included in the cell in the reference board matched with each symbol included in the cell of the matching board in Figure 24C is stored in the place in which the symbol included in the cell of the matching board is stored. Here, the sequence of the symbols stored in one row is a matched sequence.

Figure 25D shows a result that the symbol included in the cell in the reference board matched with each symbol included in the cell of the matching board in Figure 24D is stored in the place in which the symbol included in the cell of the matching board is stored.

Figure 25E shows a result that the symbol included in the cell in the reference board matched with each symbol included in the cell of the matching board in Figure 24E is stored in the place in which the symbol included in the cell of the matching board is stored.

Figure 25F shows a result that the symbol included in the cell in the reference board matched with each symbol included in the cell of the matching

board in Figure 24G is stored in the place in which the symbol included in the cell of the matching board is stored.

The last row of Figure 25F includes the special symbols in one row. When the remaining symbols are sequentially aligned except for the first symbol in the row including the special symbol, the system recognizes "1528" as the password inputted by the user. At this time, the first symbol in the row including the special symbol is the symbol included in the password. For example, when selecting the cell include din the matching board, there is an engagement between the user and the system for selecting the cell including the first symbol in the password, the system may recognizes the sequence of the remaining symbols including the first symbol in the row including the special symbol as a password.

In the method for inputting the password by matching the cell selected by the user in the matching board with the password symbol, the method that the system determines the password inputted by the user not by the method of Figure 20 is included in the scopes of the known art that a person skilled in the art well understands.

6) Modified examples

Figures 26 and 27 show the modified examples of the first embodiment

of the present invention. Figure 26 shows an example that the reference board and the matching board are overlapped in a straight line shape in parallel, and Figure 27 shows an alignment in which the straight line shaped matching board is overlapped with the matrix shaped reference board.

As shown in Figure 26A, it is possible to align the reference board and the matching board in parallel in such a manner there are not overlapped with each other. Here, matching the cell of the reference board and the cell of the matching board are performed in the same row.

The matching method for inputting the password is implemented in the same method as the above method. In the case that the password is "1528", the user selects a certain cell, for example, 8 in the matching board and sequentially matches the cells including the password of the reference board as shown in Figures 26B through 26E using the selected cell. 8 of the matching board is last matched with the special symbol * displayed in the reference board.

As shown in Figure 27A, the circulating rows are aligned in multiple, and the straight line shaped matching boards are overlapped with the reference board having the matrix shape based on the widths of the reference board.

The matching method for inputting the password is similar with the above method. In the case that the password is "1528", the user selects a certain cell, for example, the first cell in the matching board, and the cells

including the password of the reference board are sequentially matched using the selected cell as shown in Figures 27B through 27E, and the first cell of the matching board is last matched with the special symbol * displayed in the reference board.

As described above, in the password system according to a first embodiment of the present invention, the reference board and the matching board are overlapped or separated and are shown on the user interface. The reference board and the matching board each are formed of at least more than two cells. The matching board reacts with respect to the computation of the user, and the reference board reacts with respect to the computation of the user. The user selects a certain cell in the matching board, and inputs the password in such a manner that the selected cell is matched with the cell including the password symbol in the reference board. At this time, the other cells of the matching board and the other cells of the reference board are concurrently matched in multiple numbers. Therefore, others do not know the cells matched with the cells including the password symbols among a plurality of matched pairs of cells of the matching board and reference board, so that it is impossible to know the password even when the others see the input procedure of the password.

In the above description of the first embodiment of the present invention,

the matching board reacts with respect to the computation of the user, and the reference board does not react with respect to the computation of the user. However, in another embodiment of the present invention, the reversed cases may be possible. The user selects a certain cell in the matching board, and the selected cell is matched with the cell including the password symbol in the reference board for thereby inputting the password. The reversed cases may be possible. Various modifications from the first embodiment of the present invention are possible, but are obvious to a person skilled in the art, so that the detailed examples are omitted.

2. Second embodiment – password system for inputting password by selecting certain matched cell

Figures 28 and 29 are flow charts of a procedure of selecting a cell in the reference board matched with the password symbol in the matching board and inputting the password.

Figure 28 is a flow chart of a procedure for selecting a cell in the reference board matched with the password symbol in the matching board and inputting the password in the case that the system knows the length of password. Referring to Figure 28, assuming that the password of the user is P_1 $P_2 \ldots P_n$, the system shows the matching board and the reference board on the

user interface (S502). The system enables the matching board to disappear from the user interface (S503). The user repeats the procedure for selecting the cell in the reference board matched with the cell including the password symbol Pi in the matching board in the step S502 in a state that the matching board is disappeared from the user interface (1<I<n) (S504).

Figure 29 is a flow chart of the procedure for inputting the password by selecting the cell in the reference board matched with the password symbol in the matching board in the case that the system does not know the length of password. Referring to Figure 27, it is assumed that the password of the user is $P_1P_2...P_n$. The system shows the matching board and the reference board on the user interface (S602). The system enables the matching board to disappear from the user interface (S603). The user repeats the procedure for selecting the cell in the reference board matched with the cell including the password symbol P_i in the matching board in the step S502 in a state that the matching board is disappeared from the user interface (1<I<n) (S604). The user informs the system that the password input is completed (S607).

In the method of Figures 28 and 29, it is not needed that the system shows the matching board and the reference board on the user interface n-times. For example, it is assumed that the user's password is $P_1P_2...P_n$, and n represents the even number. When the system meets the j-th matching board

and the reference board on the user interface ($1<j<n/2$), the user sequentially selects the cells in the reference board matched with the password symbols P_{2j-1} and P_{2j} in the j-th matching board. Two passwords are inputted when the matching board meets with the reference board one time. Therefore, in the method for inputting the password by selecting the cell in the reference board matched with the password symbol in the matching board, when the matching board and the reference board are shown in the user interface, it is recognized that the number of the password symbols inputted by the user is promised between the user and the system.

In the method of Figures 28 and 29, when the system shows the matching board and the reference board on the user interface, it is preferred that the cell in the matching board is matched with the cell in the reference board based on a 1:1 matching method. Therefore, all cells of the matching board are matched with all cells of the reference board, so that the others who do not know the password symbols do known know the cells including the password symbols in the matching board matched with the cell selected by the user in the reference board even when the others see the procedure of inputting the password by the user.

In the method of Figures 26 sand 27, it is preferred that the password symbols in the matching board are shown in a certain non-recovering extraction

sequence. Even when they are not shown in the sequence, it does not matter. The user selects the cell in the reference board matched with the cell including the password symbol in the matching board, it is not needed that all cells in the reference board are different. In the case that they are all same, the user may confuse for selecting a certain cell, so that it is not preferred that all cells are same.

In the method of Figures 27 sand 28, selecting the cell in the reference board matching with the cell including the password symbol in the matching board is performed using the input apparatus.

In the method of Figure 29 wherein the system does not know the length of password, the user may transfer a signal that the password input is completed using the input apparatus to the system. For example, the user may use the left button of the mouse for selecting the cell in the reference board matching with the cell including the password symbol in the matching board, and the user may use a right button of the mouse for informing the completion of the password input to the system.

In the method of Figures 28 and 29, since the user selects the cell in the reference board matched with the cell including the password in the matching board, the cell including a certain password symbol must be provided in the matching board. For example, assuming that the password symbol is a

number between 0 and 9, there should be a cell including a certain number between 0 and 9 in the matching board.

In the method of Figures 28 and 29, as an example for disappearing the matching board from the user interface, it is needed to inform the position of the cell including the password symbol in the matching board to the system or it is possible when the time set in the system is passed. Assuming that Figure 30A shows the matching board, and Figure 30B shows the reference board, Figure 30D shows that the matching board is disappeared from the state of Figure 30C in which the matching board and the reference board are shown on the user interface.

Figure 31 is a flow chart of the operation of the system based on the operation of Figure 28. Referring to Figure 28, the system shows the matching board and the reference on the user interface (S701). The system disappears the matching board from the user interface (S702). When the user selects the cell in the reference cell, the symbol included in the cell in the matching board matching with the cell selected in the step S701 is recognized as the password symbol.

Figure 32 shows a procedure for determining the password symbol. It is assumed that the system shows the matching board and the reference board on the user interface as shown in Figure 32A, and Figure 32B shows a state that

the matching board is disappeared from the user interface. In addition, it is further assumed that the password symbol that the user wants to input is 6. The user selects the cell in the reference board shown in Figure 32B matching with the cell including the symbol 6 in the matching board in Figure 32A. Here, the user selects the cell including the symbol 2 of Figure 32B, and the system determines the password symbol that the user wants to input the symbol 6 in the cell including the symbol 6 matching with the cell including the symbol 2 in the reference board in Figure 32A.

Figure 33 shows a modified example of the second embodiment of the present invention and is an example that the reference board and the matching board are not overlapped and are aligned in parallel. In the case that the reference board and the matching board are not overlapped and are aligned in the straight line shape, it is known that it is possible to input the password in the same manner as the above method.

3. Third embodiment – password system for inputting password based on matching with certain cell

In the description of the third embodiment of the present invention, the method for inputting the password by matching a certain cell will be first described. Second, an actual image reference symbol set and an actual image

matching symbol set forming the two-password will be described. Third, the user interface proper to the two-password input method will be described. Fourth, the password system adapting the above password input method and the password authentication process will be described.

1) Password input method by matching of cells

In the third embodiment of the present invention, the user matches a certain cell of the reference board and the matching board based on a certain matching rule, and the password input is performed by repeating the matching process at least more than one time. At this time, in order to disguise the specific pairs of the cells matched for the password input, a false matching of each pair of cells are performed. Therefore, a plurality of cells are mixed and matched, so that even when the password input procedure is seen by others. It is impossible to recognize the actual cell matching for inputting the password, so that others cannot know the password.

Figures 34A and 34B are views for describing the password input method according to a third embodiment of the present invention. Figure 34A shows the reference board and the matching board before the matching, and Figure 34B shows the reference board and the matching board after the matching.

As shown therein, there are provided a reference board 1 formed of a plurality of cells on the upper side of the same, and a matching board 2 formed of a plurality of cells in a lower side of the same. Here, the numbers of the cells aligned in the reference board 1 are sequential, and the numbers of the cells aligned in the matching board 3 are non-sequential. The symbol board 1 and the matching board 3 may be displayed on type of the graphic user interface on a display apparatus.

The user inputs a password in such a manner that a specific cell in the symbol board 1 is matched with a specific cell in the matching board 3 based on a certain matching rule. The matching rule is directed to aligning the cells of the symbol board 1 and the matching board 3 in the same vertical row.

Assuming that the cells to be matched for the password input are 3 of the symbol board 1 and 5 of the patching board 3, as shown in Figure 34A, 3 of the symbol board 1 and 5 of the matching board 3 are not aligned vertically to each other before the matching is performed. In the drawings, 3 of the symbol board 1 and 5 of the matching board 3 are specially hatched for an easier understanding. In the actual case, there are shown in the same type as the other cells on the user interface.

The user circulates the matching board 3 four times (or five times in the left circulation direction) in the right direction for the password input, and as

shown in Figure 34B, 3 of the symbol board 1 and 5 of the matching board 3 are aligned in the same vertical row. At this time, the pairs of the cells 5 matched in the vertical row in the symbol board 1 and the matching board 3 are formed (1,2), (2,9), (3,5), (4,7), (5,6), (6,1), (7,3), (8,4), and (9,8). The total number of the same is 9. The above pairs are all number pairs obtained when moving the matching board 3 four times in the right circulation direction. However, the actually matched pairs of cells are (3,5) for the password input, and the remaining eight pairs of the cells are used for disguising the actually matched pairs of the cells (3,5).

The above matching is performed at least more than one time during one time password authentication. Therefore, even when the password input procedure is exposed to the others, the others cannot recognize the password inputted. The authentication process of the password inputted in the above manner will be described.

Figure 35 is a view for describing the password input method according to a third embodiment of the present invention implemented based on the common set concept. Referring to the drawings, assuming that there are the sets having a n number of numbers (n is natural number) as the elements of the set, the user selects one element of the set A and one element of the set B for the password input and matches the selected two elements. In addition, at this

time, the other elements of the sets A and B are matched with each other based on a certain matching rule.

As a method for matching two cells of two sets A and B, there is a method for changing the aligned sequences of the elements belonging to a certain set. For example, the aligning sequence of the elements of the set B is changed. Therefore, a set C of the matched elements is generated based on a certain matching rule between the set B having the changed aligning sequence and the set A.

The matching method of the above elements will be described based on a password input process. First, in a step S1, each element of the sets A and B is provided. In a step S2, the aligned sequence of the elements of the set B is changed. In a step S3, a set C formed of a pair of matched elements is generated based on a matching sequence of the elements of the set A and the set B'. An authentication is achieved based on the generated set C.

Here, a certain element of the set A that is a reference for the matching is called as a real reference cell (RRC), and the remaining elements for disguising the RRC is called as a virtual reference cell (VRC). A certain element of the set B for matching to the RRC is called as a real matching cell (RMC). The remaining elements for disguising the RMC are called as a virtual matching cell (VMC). For example, as shown in Figures 36A and 34A, there are provided

a real reference cell and a virtual reference cell, and a real matching cell and a virtual matching cell used in the reference board and the matching board, respectively.

When the RRC of the set A and the RMC of the set B are matched, the VRC of the set A and the VMC the set B are matched. The pairs of the sets C that the set A and the set B are matched based on a certain matching rule are called as a matched cells group (MCG). For example, as shown in Figures 36B and 34B, there are shown the real matched RRC and RMC, and the virtual matched VRC and VMC, and the MCG in the pairs of the matched cells.

In addition, the matching of the RRC and the RMC is performed by at least more than one time. As shown in Figures 37A through 37D, a plurality of cell matching procedures are repeatedly performed for thereby inputting a password. As shown therein, the hatched symbols are provided for helping a better understanding of the descriptions. They are shown on the user interface in the same shape as the other symbols.

In each drawing, the contents in the upper sides are the reference board 7 and the matching board 9 for showing the after-matching state with respect to the before-matching contents of the lower side. In the matching rule, the RRC of the symbol board 7 and the RMC of the matching board 9 are aligned in the same vertical row. For example, assuming that the RRC is 3, 7, 2,

9 and the RMC is 5, 1, 6, 6, in order to match with the RRC and RMC, as shown in Figures 37A through 37D,3 and 5, 7 and 1, 2 and 6, and 9 and 6 are sequentially matched using the symbol board 6 and the matching board 9.

Here, the group of the symbols formed of a plurality of RRC is called as a real reference cell group (RRCG), and the group formed of a plurality of RMC is called as a real matching cell group (RMCG). Here, the RRCG is 3729, and the RMCG is 5166.

In the password input method according to a third embodiment of the present invention, when one RRC and RMC are matched, a plurality of VRC and VMC are matched. Therefore, a third party person who watches the input procedure of the password cannot recognize which symbol matching corresponds to the RRC and RMC for thereby preventing a leakage of the password.

In the above examples, the number of the cells including the RRC and VRC is the same as the number of the cells including the RMC and VMC (in the embodiment, the number of the same is 9), but they are not needed to be same. Namely, they may be different in another embodiment of the present invention. For example, the number of the symbol rows aliened in the upper side may be 9, and the number of the symbol rows aligned in the lower side may be 7.

2) Generation of two passwords, and RRCG and RMCG

Since the password used in a password input method of a third embodiment of the present invention is different from a password used in the common password system, the password used in the third embodiment of the present invention is called as a two-password.

The password used in the common password system is a symbol group in which symbols are sequentially aligned. Therefore, it is needed to sequentially input the password in a determined sequence based on the symbol group designed as a password into the password system. For example, in the case that the password of a credit card is set as 2976, when it is intended to use the credit card in an automatic teller machine (ATM), the user should sequentially input 2, 9, 7 and 6 using the number keypad provided in the ATM.

However, the two-password has different from the conventional password of the above input method. The two-password may be formed of RRCG and RMCG. The two-password may be either RRCG or RMCG or may be induced from the same. Therefore, what the symbol group formed of RRCG and RMCG is called as the two-password. In detail, various methods for determining the RRCG and RMCG from the two-password will be described with reference to Figures 38A through 38D and Figures 39A and 39B.

First, an example that the two-password is formed of RRCG and RMCG

will be described. For example, when the two-password is 37295166, the front side four numbers of 3729 are defined as RRCG, and the rear side four numbers of 5166 are defined as RMCG. In this case, the sequential pairs of the real matched RRC and RMC are (3,5), (7,1), (2,6), and (9,6). The method for generating the RRCG and RMCG from the two-password may be implemented follows. As shown in Figure 38A, in the case that the two-password is defined, the RRCG and RMCG are as follows. The sequential pairs of the RRC and RMC are implemented as follows.

Two-password: $X_1\ X_2\ X_3\ \ldots\ X_{n-2}\ X_{n-1}\ X_1\ X_1\ X_2\ X_3 \ldots\ X_{n-2}\ X_{n-1}\ X_n$ (n is natural number)

RRCG: $X_1\ X_2\ X_3 \ldots\ X_{n-2}\ X_{n-1}\ X_n$

RMCG: $Y_1\ Y_2\ Y_3 \ldots\ Y_{n-2}\ Y_{n-1}\ Y_n$

The sequence pairs (RRC_i, RMC_i) of RRC and RMC: (X_i, Y_i) $(1 \le l \le n)$

Second, an example that the two-password is formed of RRCG and RMCG will be described.

The RRCG and RMCG are formed using the groups of the numbers alternately selected from the two-password. For example, when the two-password is 37295166, the RRCG and RMCG are 3256 and 7916, respectively.

In this case, the sequence pairs of the RRC and RMC real-matched for the input of the password is (3,7), (2,9), (5,1), (6,6). The method for generating the RRCG and RMCG from the two-password may be implemented as follows. As shown in Figure 38B, in the case that the two-password is defined, the RRCG and RMCG are as follows. At this time, the sequence pairs of the RRC and the RMC may be expressed as follows.

Two-password: $X_1\ Y_1\ X_2\ Y_2\ X_3\ Y_3 \ldots X_{n-2}\ Y_{n-2}\ X_{n-1}\ Y_{n-1}\ X_n\ Y_n$ (n is natural number)

RRCG: $X_1\ X_2\ X_3 \ldots X_{n-2}\ X_{n-1}\ X_n$

RMCG: $Y_1\ Y_2\ Y_3 \ldots Y_{n-2}\ Y_{n-1}\ Y_n$

The sequence pairs of the RRC and RMC $(RRC_i, RMC_i) : (X_i, Y_i)\ (1 \le i \le n)$

Third, in the case that the two-password is RRCG, the RMCG is induced from the above two-password. For example, when the two-password is 37295166, the entire number group of the same is used as the RRCG, and the RMCG is induced therefrom. For example, the inducing rule is to use the number group obtained by rotating the RRCG one time. In this case, the RMCG becomes 72951663. The sequence pairs of the real-matched RRC and RMC for the input of the password is (3,7), (7,2), (2,9), (9,5), (5,1), (1,6), (6,6), (6,3). The

method for generating the RRCG and RMCG from the two-password will be implemented as follows. As shown in Figure 38C, in the case that the two-password is defined, the RRCG and RMCG are as follows. At this time, the sequence pairs of the RRC and RMC are implemented and expressed as follows.

Two-password: $X_1\ X_2\ X_3 \ldots\ X_{n-2}\ X_{n-1}\ X_n$ (n is natural number)

RRCG: $X_1\ X_2\ X_3 \ldots\ X_{n-2}\ X_{n-1}\ X_n$

RMCG: $X_2\ X_3 \ldots\ X_{n-2}\ X_{n-1}\ X_n\ X_1$

The sequence pairs of the RRC and RMC (RRC_i, RMC_i) : (X_i, X_{i+1}) ($1 \le i \le n-1$), (X_i, X_1) ($i=n$)

Fourth, a part of the two-password is RRCG. Another part including a part of the RRCG is RMCG. For example, when the two-password is 37295166, the remaining group 3729516 except for the last number is used as RRCG. The remaining group 7295166 except for the first number is used as RMCG. The sequence pairs of the real matched RRC and RMC for the input of the password is (3,7), (7,2), (2,9), (9,5), (5,1), (1,6), (6,6). The method for generating the RRCG and RMCG from the two-password may be implemented as follows. As shown in Figure 38D, the two-password may be defined, and the RRCG and

RMCG may be defined as follows. At this time, the sequence pairs of the RRC and RMC may be implemented as follows.

Two-password: $X_1X_2X_3\ldots X_{n-2}\ X_{n-1}\ X_n$ (n is natural number)

RRCG: $X_1\ X_2\ X_3\ldots X_{n-2}\ X_{n-1}$

RMCG: $X_2\ X_3\ldots X_{n-2}\ X_{n-1}\ X_n$

The sequence pairs of the RRC and RMC $(RRC_i, RMC_i) : (X_i, X_{i+1})$ $(1\leq i\leq n-1)$

As described above, there are various methods for generating RRCG and RMCG from the two-password. The RRCG and RMCG generated from the two-password have a relationship of 1:1. They may have a relationship of 1:n or n:1. For example, as shown in Figures 39A and 39B, only one RRC is generated as RRCG from the two-password, and the remaining symbol group is generated as RMCG. In addition, the reverse generation is also possible. At this time, the sequence pairs of the RRC and RMC may be expressed as follows.

The sequence pairs of RRC and RMC $(RRC_i, RMC_i) : (X_1, X_{i+1})$ $(1\leq i\leq n-1)$

The sequence pairs of RRC and RMC $(RRC_i, RMC_i) : (X_i, X_n)$ $(1\leq i\leq n-1)$

The method for generating RRCG and RMCG from the two-password, and the method for forming a sequence pair of RRC and RMC may be modified and applied in various methods. The above various modifications and applications are obvious to a person skilled in the art. The other modification and applications described in the present description may be included in the concept of the present invention. In addition, in the basic application of the two-password, the three-password is also possible, and the four-password or the more passwords are also possible. The above applications and extensions should be implemented in considered with the users. Namely, memorizing the two-password should be easy to the users, and the procedure for matching the symbols for inputting the two-password should be easy.

3) User interface and password system for two-password input

The password input method based on the matching of cells may be implemented based on a password system having a user interface and a password authentication process.

Figure 40 is a block diagram showing a relationship between the password system and a main system adapting the same according to a preferred embodiment of the present invention. The password system 30

provides a user interface 20 so that a user 10 can input a two-password. The user interface 20 includes interface members for inputting the two-password by the matching of cells by the user. The password system 30 receives the two-password inputted from the user through the user interface 20 and performs an authentication and enables the authenticated person to access the main system 40.

The user interface 20 is not limited to a few embodiments to be described later. The detained embodiments of the user interface 20 that will be described later are provided for only easier understanding of the present invention. Various modifications and applications of the detailed constructions of the user interface 20 based on the characteristics of the main system 40 adapting the password system 30 are obvious to a person skilled in the art. For example, in the case that the password system 30 is mounted on a personal computer system, the user interface 20 may include a graphic user interface. In the case that it is mounted on an electrical door lock system, the user interface 20 may include a mechanical system and an electronic circuit.

In detail, the constructions of the user interface 20 and the password system 30 will be described. Figure 41 is a view illustrating the basic construction of the user interface for the password system according to the present invention, and Figure 42 is a flow chart illustrating a user authentication

process of the password system of the present invention.

The two-password system 30 according to the present invention includes a display control unit 31, a cell generation unit 32, a matching cell process unit 33, an authentication process unit 34, and a memory 35. The user interface 20 for the two-password input includes a display unit 22 and a matching unit 24.

As shown in Figures 41 and 42, in a step S10, the cell generation unit 32 generates a group of cells included in each cell of the reference board and the matching board displayed on the display unit 22 and provides the group to the display control unit 31. In a step S20, the display control unit 31 includes the provided symbol group into the cells of the reference board and the matching board and outputs to the display unit 22, so that the reference board and the matching board are displayed on the display unit 22.

In a step S30, the user 10 matches the cells of the reference board and the matching board displayed on the display unit 22 using the matching unit 24. In a step S40, the matching cell process unit 33 generates a matched cell group MCG based on the input of the user through the matching unit 24. In a step S50, the generated group is inputted into the authentication process unit 34. In a step S60, the authentication process unit 34 performs a password authentication process based on the authentication reference information 36 stored in the

memory 35. The detailed process thereon will be described later.

In the password system, the group of the cells for inputting the two-password is generated and displayed to the user differently from the conventional password system. In addition, the authentication process based on the matched cell group MCG is different t from the conventional password system in their characteristics. The detailed descriptions thereon will be provided later.

The detailed embodiments of the user interface 20 based on the main system 40 will be described with reference to Figures 43 through 55.

Figure 43 is a view illustrating an embodiment of the user interface based on the main system according to the present invention. The password system 30 may be mounted on the main system 40 such as a system having a graphic user interface, for example, a personal computer system, PDA, ATM financial terminal, etc. At this time, the user interface 20 includes the display apparatus 50 as a display unit 22 such as a CRT display apparatus, a LCD apparatus, etc., and the graphic user interface 60. In addition, there is further provided an input apparatus 54 as a matching unit 24 such as a keyboard apparatus, a pointing apparatus, etc.

The graphic user interface 60 displayed on the screen 52 of the display apparatus 50 includes a reference board 61 and a matching board 62. The user

10 uses an input apparatus 54 for inputting the two-password. The cells aligned on the reference board 61 and/or the matching board 62 are circulation-moved in accordance with a control of the user 10.

In the circulation display method, the reference board 61 may be fixedly displayed, and the matching board 62 may be circulated in the right or left direction. In addition, since the symbol row aligned on the reference board 61 is a reference for the matching, it is preferred that a display sequence is sequentially displayed so that the RRC is quickly recognized. However, there is a certain complexity so that the user can easily recognize the RRC, the aligning sequence of the reference board 61 may be randomly displayed in a non-sequence. It is preferred that the symbols aligned on the matching board 62 are randomly displayed based on a non-recovering method.

In another method of the circulation display, the reference board 61 and the matching board 62 may be circulated and displayed in different directions. However, in the case that there is a certain complexity so that the user can easily recognize the RRC, the aligning sequence of the reference board 61 may be randomly displayed based on the non-sequential method. It is preferred that the symbols aligned on the matching board 62 are randomly displayed.

In another circulation display method, the reference board 61 and the matching board 62 may be circulated and displayed in different directions. The

reference board 61 may be fixedly displayed, and each cell of the matching board 62 may be circulated and displayed, being moved from its original place to the upward side or downward side. The above circulation display method may be modified and applied in various methods in addition to the above-described method. The above applications and modifications are obvious to a person skilled in the art.

In the display type of the cells, the reference board 61 and the matching board 62 may be displayed in a straight line shape and may be displayed in various shapes. For example, as shown in Figures 44A through 44D, it may have a circular shape or a matrix shape. In addition, the aligned cells may be formed in numbers, characters, graphics, pictures, and a combination of the same. In addition, the aligned cells may be displayed with a color so that a user can easily recognize. For example, the cells of the matching board 62 may have different colors in a circle having numbers. The method for selecting colors is determined so that the user can quickly recognize the symbols. There may be various applications in the display method of the cells. It is also obvious to a person skilled in the art. As it is not shown in the drawings, even when the cells are aligned randomly, when there is a certain rule in the circulation, the cells may be formed in a board.

In the case that either the reference board 61 or the matching board 62

is fixedly displayed for recognition, the display of the same may be omitted. For example, in the case that the numbers 1~9 are sequentially displayed on the reference board 61, the user can easily recognize the reference board 61, so that the display of the same may be omitted as shown in Figure 45.

In another embodiment of the present invention, as shown in Figure 46, the reference board 61 and the matching board 62 may have switched display shapes. For example, the symbols aligned on the matching board 62 may be sequentially aligned, and the sequences of the symbols aligned on the reference board 61 may be aligned randomly based on the non-recovery method. In addition, the matching board 62 may be fixed, and the reference board 61 may be circulated and displayed in accordance with a control of the user. The above modification is obvious to a person skilled in the art.

In another embodiment of the present invention, as shown in Figure 47, at least more than two matching boards 62 may be concurrently displayed in parallel. The user inputs the two-password by sequentially performing the symbol matching with the reference board 61 using each cell. The number of the cells displayed on the matching board 62 is determined by the number of the RMCG. It may be smaller than the number of the RMCG. The cells not displayed when the cells are circulated and moved may appear and may be displayed.

In the above description of the present invention, the symbol row is circulated for the symbol matching. In another embodiment of the present invention, the circulation moving distance of the symbol row may be directly inputted. As shown in Figure 48, an additional input window 63 may be provided on the graphic user interface 60, so that the circulation moving distance of the matching board 62 may be directly inputted by the user. For example, in the case that the RPCG is 3 as one RRC, and the RMCG is 5618, the numbers 5, 6, 1 and 8 of the matching board 62 are circulated in the right direction and are matched with respect to the cell 3 of the reference board 61. At this time, the circulation moving distance is 4 times, 2 times, 1 time, and 7 times. Therefore, 4217 are inputted on the input window 63.

As shown in Figure 49, a plurality of matching control buttons 64 may be provided on the graphic user interface 60 for circulating and matching the symbol row. The matching control button 64 includes a left, right circulation movement button, a start/reset button, a matching button and an input completion button.

In another embodiment of the present invention, the reference board 61 or the matching board 62 may be automatically circulated, and the user performs an input operation when the RRC of the reference board 61 and the RMC of the matching board 62 are matched. For example, as shown in Figure

50, when the matching board 62 is automatically circulated, the user may input the enter button 65 displayed on the graphic user interface 60 and informs that the symbols are matched or may input the enter key of the input apparatus 54. In the drawings, the arrow indicated by the dotted line of the matching board 62 represents a rotation direction, but is not actually displayed.

The graphic user interface is not limited to the above descriptions. At least more than two above-described embodiments may be combined. In addition, the number of the cells aligned on the reference board 61 and the matching board 62 may be limited to a certain number in consideration with the user's state and security. For example, in the case that it is intended to increase the security, it is needed to increase the number of the cells aligned, and in the case that a fast password input and process is needed, the number of the cells aligned may be decreased.

The two-password system according to the present invention may be mounted on a mechanical system and a system having an electronic circuit, for example, a locking system such as an electrical door lock, and an entrance control system. The two-password system may be cooperate with the mechanical system and electronic circuit mounted on the main system. In this case, the user interface may be constituted as follows.

Figure 51 is a view illustrating an example of a user interface of the two-

password system cooperating with the electronic circuit. Figure 52 is a view illustrating an example of displaying one matching board, and Figure 53 is a view illustrating the construction of a circuit of a user interface of Figure 51.

Referring to the drawings, the password input panel 70 is provided as a user interface for inputting the two-password in the main system 40 like the electronic door lock or entrance control system. The password input panel 70 includes a LCD 71 as a display unit for displaying the symbol group. In the LCD 71, the images of the reference board 72 for displaying the RRC and VRC and the matching board 73 for displaying the RMC and VMC are displayed. As shown in Figure 52, only the matching board 73 may be displayed on the LCD 71, and the reference board display region 72a may be provided on an upper side of the front surface of the password input panel 70 for thereby printing and displaying a corresponding cell. In addition, as a matching unit, there are provided a plurality of the matching control buttons 74 on the front surface of the password input panel 70. As the matching control button 74, there are a left and right circulation movement button, a start/reset button, a matching button, and an input completion button.

The password input panel 70 includes the LCD control circuit and the button input process circuit 75 and displays the reference board 72 and the matching board 73 on the LCD 71 in response to a display control signal

provided from the password system 30. The user inputs the two-password using the matching control button 74. The LCD control circuit and the button input detection circuit 75 receive an input of the matching control button 74 and provides to the two-password system 30.

Figure 54 is a view illustrating an example of the user interface of the password system cooperating with the mechanical system. Figure 55 is a view illustrating an example of the circuit construction of the user interface of Figure 54.

As shown in the drawings, the password input panel 80 includes a reference board display region 81 in an upper side of the front surface, and the symbols displaying the RRC and VRC are printed and displayed. The matching board for displaying the RMC and VMC includes a wheel mechanism 82 coupled with a plurality of wheels 83. A plurality of symbols are circulated and printed on each wheel 83.

The password input panel 80 includes a wheel driving and rotation degree detection circuit 85 for thereby driving the wheel mechanism 82 in response to a display control signal from the two-password system 30. The user inputs a two-password using the wheel control button 74. The wheel control button 74 is constituted in such a manner that a wheel adapted to rotate the wheel-mechanism 82 in upward and downward directions and a button adapted

to generate a matching input signal are combined. The wheel driving and rotation degree detection circuit 85 receives an input of the wheel control button 84 and provides to the two-password system 30.

The user interface of the two-password system using the wheel mechanism 82 may be implemented using the above-described graphic user interface. Namely, the reference board and/or matching board may be displayed using the graphic user interface and may be implemented based on the up and down movement method. At this time, the control of the up and down circulation movement is implemented by providing an additional input apparatus or by displaying a wheel control button on the screen.

When circulating and moving the matching board, it is possible to perform a matching input using the left or right (up or down) direction key. For example, when a certain cell of the designated matching board is matched with a certain cell of the reference board by circulating the cells in one direction, the direction conversion is performed. When the time when the conversion of the circulation direction is judged to be a matching state, it is not needed to additionally provide a button for the matching input.

As described above, the user interface for the two-password input of the two-password system according to the present invention may be implemented in various manners based on the characteristics of the main system 30. In the

user interface method not descried in the above embodiments of the present invention, the password input method based on the symbol matching may be adapted by a user skilled in the art.

4) Authentication process of password system adapting the two-password

Referring to Figures 41 and 42, the authentication process of the two-password system will be described in detail by a step-by-step method.

As shown in Figures 421 and 42, in a step S10 of the two-password authentication process, a cell generation unit 32 generates a group of the cells displayed on the display unit 22. When the cell generation unit 32 generates the cells aligned on the reference board and the matching board, the generation sequence of the cells is randomly performed based on the non-recovery method or the generation may be performed based on a determined sequence or may be performed in a combined method.

For example, the cells aligned in the matching board may be randomly generated based on the non-recovery method in a determined sequence in the case of the cells aligned in the reference board. The cells aligned in both the reference board and the matching board may be randomly generated based on the non-recovery method. The cells aligned in the matching board may be randomly generated based on the non-recovery method. The cells aligned in

the reference board may be generated by rotating the sequence of the cells aligned in the matching board.

As another example, the RRCG and RMCG are extracted based on the authentication reference information 36 stored in the memory 35, and the aligning sequence of the symbols is determined based on the extracted information. An aligning sequence of the symbols may be determined in a sequence that the user feels easy for inputting the two-password. For example, the aligning sequence of the symbols may be determined in such a manner that the rotation number of the matching board is within a certain range.

Figures 5 and 6 show an example that the cells are aligned in such a manner that the rotation number of the matching board is within a certain range. In the case that the matching board 62 is automatically rotated in the right direction, when the two-password is 134672, and the RRCG is 147, and the RMCG is 362, the group of the cells aligned in the matching board 62 is generated with 378612954.

At the initial display state, since the numbers 1 and 3, and 4 and 6 are previously matched and displayed, the numbers 1 and 3, and 4 and 6 are matched by pressing the enter button 65 by two times. When the matching board 65 is moved in the right direction by one field, the numbers 7 and 2 are matched, and then the enter button 65 is inputted. Namely, the aligning

sequence of the symbols may be determined based on the user's convenience.

However, what there is not a circulation and movement of the cells in all cell matching should be excluded. In the case of all cell matching, only when the enter button 65 is inputted, a security may be weakened. Namely, at least more than one time cell movement should be performed for obtaining a desired security. Namely, the aligning of the cells should be performed in such a manner that over circulation and movement do not occur, and a desired security is obtained. Here, the important thing is to provide a convenience in maximum when the user inputs the two-password.

In addition, in the authentication process of the two-password system, there may be provided a step for inputting a two-password and inputting an inherent ID provided to the user. For example, in the case that the main system 40 is a system having a plurality of users, it is needed to separately input the user's ID. The detailed description thereon will be provided later. In the authentication process that the user inputs an additional ID, a step may be further provided for extracting authentication reference information 36 from the memory 35 using the ID inputted.

The process for determining the symbol aligning sequence and generating a symbol group may be performed one time during the input process of the two-password or may be repeatedly performed during every cell matching.

The group of the cells generated is provided to the display control unit 31. In a step S20, the display control unit 31 outputs the group of the generated cells to the display unit 22. The display unit 20 displays the group of the cells in accordance with a control of the display control unit 31. The method for displaying the group of the cells is implemented based on one among the various embodiments of the user interface for the input of the two-password.

In a step S30, the user 10 matches the symbols displayed on the display unit 22 using the matching unit 24. In a step S40, the matching cell process unit 33 generates the matched cell group MCG based on the input by the user through the matching means 24. The example of the generation of the MCG will be described with reference to Figures 24A through 24D.

As shown in the drawings, the symbols hatched in the reference board 90 and the matching board 91 are provided to an easier understanding. When they are shown on the user interface, they are displayed in the same manner as other symbols.

In the case that the RRC is 3, 7, 2, and 9, and the RMC is 5, 1, 6 and 6, the user sequentially matches 3 and 5, 7 and 1, 2 and 6, and 9 and 6 of the reference board 90 and the matching board 91 based on the step of the matching. At this time, the generated MCG is shown in Figure 58. The MCG (MCG_1~MCG_4) generated in every step are inputted into the authentication

process means 34 in a step S50.

In the case that the sequences of the symbols aligned in the reference board 90 are determined, only the symbols aligned in the matching board 91 may be transferred to the authentication process unit 34 at the time of the matching. Here, all information of the symbols aligned in the matching board 91 with respect to only the first match are transferred, and the information concerning the rotation number of the matching board 91 is transferred from the time of the second matching. In addition, in the case that the sequences of the symbols are not determined in the reference board 90, all symbols in the reference board 90 and the matching board 91 may be transferred in a sequence at the time of the matching.

The information transferred to the authentication process unit 34 may be modified or applied in various forms based on the characteristic of the user interface. The above modification and application are obvious to a person skilled to the art. In addition, the transfer to the authentication process unit 34 may be performed one time at the time of the completion of the password input. Whenever one time patching is performed, the transfer may be implemented.

In a step S60, the authentication process unit 34 performs a password authentication process based on the authentication reference information 36 stored in the memory 35. The flow chart showing the detailed process of the

password authentication process is shown in Figure 59.

As shown in Figure 59, the authentication process means 34 received the MCG from a step S61. The authentication reference information 36 is patched from the memory 35 in a step S62. In this embodiment of the present invention, the authentication reference information is a two-password. In a step S63, the RRCG and RMCG are induced from the two-password. In a step S64, the cells matched with the RRCG induced from the two-password are determined by the MCG. For example, as shown in Figure 60, in the case that the RRCG is 3729, the symbols of the MCG matched are 5, 1, 6, and 6.

In a step S65, the symbol group determined in the MCG and the RMCG induced by the two-password are compared. In a S66, it is judged whether two symbols are matched. In the case that they are matched, in a step S67, the system access is allowed, and in the case that they are not matched, the system access is denied in a step S68.

Here, the authentication reference information stored in the memory 35 may be a two-password or may be separated into the RRCG and MMCG and stored or one of the RRCG and MMCG may be stored. For example, as shown in Figure 5C, when forming the RRCG and RMCG, the RRCG is stored, and the RMCG is induced and used. In the case that the user ID is inputted in the authentication process, the authentication reference information 36 may be

patched from the memory 35 based on the ID inputted.

The authentication process of the two-password system may be adapted to a single user system. In the case of a plurality of user systems, there is further provided a step for inputting the two-password and the user ID. As shown in Figure 61, the authentication process unit 34 patches a corresponding authentication reference information 37 stored in the memory 35 based on the user ID.

In the case of a plurality of user systems, the authentication process may be performed without an additional user ID input. For example, as shown in Figure 62, the inputted MCG may be applied as an index. Here, the cell generation unit 32 patches the authentication reference information using the MCG. The method for inputting a user ID may be implemented using an input apparatus or a button in the graphic user interface. In addition, the single user system may include a process for inputting a user ID.

5) Application of password system adapting two-password

The password system according to the present invention may be adapted to any type of system requiring the password input. For example, the present invention may be well adapted to a personal computer system, a locking system, an ATM financial terminal, a PDA, a cellular phone, an internet

banking system, a cyber trading system, etc.

The case that the password system 30 of the present invention is mounted on the standalone system 100 is shown in Figure 63. The user interface 20 of the two-password system 30 mounted on the standalone system 100 may be installed in an internal type or an external type. For example, in the case of the personal computer system, the user interface 20 may be formed of the graphic unit interface or the input apparatus or a combination of the same.

Figure 64 is a view illustrating an example that the two-password system of the present invention is mounted on the main system under the network environment, and Figure 65 is a view illustrating an example that the password system is mounted on the communication terminal under the network environment.

The password system of the present invention may be used under the network environment. As shown in Figure 64, the password system 30 may be mounted on the main system 40 connected through a communication network 120. The communication terminal 110 receives a group information of the cells from the main system 40 through the communication network 120 and displays using the user interface 20, and the user inputs a two-password using the user interface 20. The information occurring by the input of the two-password, for example, the matched cell group MCG is inputted into the two-password system

30 mounted on the main system 40 through the communication network 120 by the communication terminal 110. The information transferred from the communication terminal 110 to the main system 40 may be transferred by a certain amount as much as the circulation movement distance of the cell during the cell matching.

The transferring information may be encrypted or may be coupled with a security platform. Here, the information transferred may include a user ID information. In the case that the MCG has the functions of the index, for example, in the case that only the user ID is shown, only the MCG is transferred. Various other modifications are possible.

In the case that the user ID is stored in the communication terminal 110, the user inputs only the two-password, and an additional ID input process may be omitted. At this time, the two-password system 30 mounted on the main system 40 may perform the patching of the two-password, real reference cell group and real matched cell group in the memory using the user ID provided from the communication terminal 110.

In another embodiment of the present invention, as shown in Figure 65, the two-password system 30 may be mounted on the communication terminal 110. In this case, the authentication process is performed by the communication terminal 110.

As described above, in the two-password system 30 according to the present invention, the user interface 20 and the other elements as shown in Figure 41 may be mounted on the standalone system 200 or the communication terminal 110 connected with the communication network by a wired or wireless or computer network method or may be mounted on the main system 40. A part of the elements may be separated and separately constituted. For example, the memory 35 adapted to store the authentication reference information 36 may be provided in the communication terminal 110 or the main system 40.

In the above embodiments of the present invention, only the matching of the symbols is adapted as examples. In the matching method of the present invention, one picture may be assembled like a picture puzzle or a special number may be assembled based on a two-password input method.

Industrial Applicability

In the password input method and system based on the matching of cells of the present invention, even when the password input procedure is directly exposed to others, the other cannot recognize the cells matched for the password input among a plurality of matched cell pairs provided in the matching board and the reference board. Therefore, in the present invention, it is possible to prevent the password from being revealed to others who watched the

password input procedure. In addition, it is possible to overcome a user's uneasiness during a password input and to enhance a security of the system.

As the present invention may be embodied in several forms without departing from the spirit or essential characteristics thereof, it should also be understood that the above-described examples are not limited by any of the details of the foregoing description, unless otherwise specified, but rather should be construed broadly within its spirit and scope as defined in the appended claims, and therefore all changes and modifications that fall within the meets and bounds of the claims, or equivalences of such meets and bounds are therefore intended to be embraced by the appended claims.